



CLIENT ALERT

**New California Online Privacy Protection Act Requires Privacy Notices for all Website Operators**

Daniel L. Appelman, Silicon Valley

In mid-October, Governor Gray Davis signed the Online Privacy Protection Act of 2003 ("OPPA"). The new law will take effect on **July 1, 2004** (unless preempted by federal legislation, FTC regulations, or court action) and will become part of the Business and Professions Code at §§ 22575 through 22579. OPPA will require every person and business entity in the United States (and presumably anywhere in the world) that owns a website and collects personal information about California residents to post a conspicuous privacy policy on that website stating what information they collect and with whom they share it, and to comply with that policy. Violations of the new law can result in civil penalties and can be the basis for suits brought by the California Attorney General as well as by private individuals.

Federal law generally does not require websites to include privacy policies, although there are exceptions related to the banking and health services industries and to websites directed to children. The new California law is one of several recent examples where the California legislature has gone further than Congress in imposing significant restrictions on the way companies, regardless of where they are located, conduct their business

online or with the aid of computers, to the extent such business practices affect California residents.¹ Compliance with OPPA is not intuitive, and companies must become familiar with its particular requirements.

Who Must Comply

The new law applies to all "operators" of commercial websites and online services that collect personally identifiable information about California consumers. This includes out-of-state operators as well as those based in California.

The term "operator" means the owner of a website or an online service. It does not include third parties that may operate, host or manage the site or service or who process information on behalf of the owner. The term "personally identifiable information" means individually identifiable information collected online about individual consumers, such as a first and last name, a street address, an e-mail address, a telephone number, a social security number or any other identifier that would permit the operator, or others who obtain access to that information, to contact a specific individual. The term "consumer" means any individual who seeks or acquires goods, services, money or



Daniel L. Appelman advises clients on technology issues and transactions, including joint ventures, strategic alliances, technology transfers and licensing.

He also counsels clients on compliance with technology-related laws and regulations, such as those addressing spam, privacy, intellectual property infringement, government procurement and export control. Dan is the chair of the State Bar of California's Cyberspace Law Committee and frequently publishes articles and speaks on technology issues. For more information on Mr. Appelman's practice, contact him at 650.324.6706 or dappelman@hewm.com

Office Locations

San Francisco
333 Bush Street
San Francisco, CA 94104-2878
415.772.6000

Silicon Valley
275 Middlefield Road
Menlo Park, CA 94025-3506
650.324.7000

Silicon Valley
2775 Sand Hill Road
Menlo Park, CA 94025-3506
650.854.4488

Los Angeles
601 South Figueroa Street
40th Floor
Los Angeles, CA 90017-5758
213.689.8400

San Diego
4350 La Jolla Village Drive
7th Floor
San Diego, CA 92122-1246
858.450.8400

Seattle
701 Fifth Avenue
Suite 6100
Seattle, WA 98104-7098
206.447.0900

credit for personal, family or household purposes. OPPA does not apply to owners of websites that only collect information about other businesses.

What the New Law Requires

The new law requires an operator to conspicuously post a privacy policy on its website, or in the case of an online service, to use reasonable means to make that policy available to consumers. In order to meet the “conspicuously posted” requirement:

- The privacy policy must appear prominently on the home page of a website;
- The privacy policy must be directly linked to the home page by means of an icon that contains the word “privacy” and uses a color that contrasts with the background of the web page; or
- The privacy policy must be linked to the home page by means of a hypertext link that includes the word “privacy,” is written in capital letters equal to or greater in size than the surrounding text, or is otherwise readily distinguishable from the surrounding text on the home page.

The privacy policy itself must do all of the following:

- It must identify the categories of personally identifiable information that the operator collects;
- It must identify the categories of third parties with whom the operator may share the personally identifiable information that it collects;
- It must describe the process (if any) by which consumers can review and request changes to any of the collected information;

- It must describe the process by which the operator will notify consumers of material changes in its privacy policy; and
- It must identify the effective date of the privacy policy.

OPPA contains a built-in “cure period” — it expressly provides that an operator who has been notified that it is not complying with the requirement to post its privacy policy will not be considered in violation of the law unless it fails to post its privacy policy within 30 days of such notification. Other provisions of the new law indicate that an operator intentionally failing to comply with the law will be considered in violation of OPPA even if the noncompliance is immaterial, while an operator whose noncompliance is not intentional, but negligent, will only be considered in violation of OPPA if the noncompliance is material.

The Consequences of Not Complying

The new law does not itself contain enforcement provisions. It is expected that OPPA will be enforced through California’s Unfair Competition Law (the “UCL”), which is located at Business and Professions Code §§ 17200-17209.

Under the UCL, the Attorney General, district attorneys, and certain city and county attorneys may bring civil actions based on acts of “unfair competition” as defined in Business and Professions Code § 17200. Acts of “unfair competition” include acts, in business, that violate any law, which means that once OPPA takes effect in July 2004, a violation of OPPA will also be a violation of the UCL. The identified law enforcement officials may seek civil penalties and injunctive or other equitable relief.

Of greater concern, under the UCL “any person” may bring an action “in the interests of itself, its members, or the general public.” This “private attorney general” provision has

been broadly interpreted to allow a person with no personal interest and who has suffered no harm to bring a private action for restitution (to be paid to those who have suffered harm) or injunctive relief.² In a private attorney general action brought under this special standing provision, the plaintiff may also recover attorney's fees. Therefore, private plaintiffs will be able to use alleged violations of OPPA as a basis for asserting private UCL claims.

Recommendations

We recommend that companies start planning now to comply with the new law. Even if OPPA is preempted or overturned, posting a privacy policy and complying with it is becoming standard practice for those doing business on the Internet. Those privacy policies should disclose:

- What information website operators collect from those visiting their sites;
- How that information is used;
- With whom it is shared;
- How consumers can review and correct the collected information;
- Whether consumers can “opt out” of having that information retained by the operator or shared with others; and
- How consumers can communicate with the operator.

Please contact us if you would like our help in drafting a privacy policy tailored to your unique business needs, or to review your current policy for compliance with California's new law.

Footnotes:

¹ Other examples include a new law requiring companies to maintain databases that include personal information about California residents to disclose any breach in security of those databases, which became effective on July 1, 2003; and a broad prohibition against sending unsolicited commercial e-mail messages (“spam”) to California e-mail addresses, which will become effective January 1, 2004.

² Heller Ehrman has a primer available on the UCL. Please contact us for a copy if you are interested in learning more about this law.

Office Locations

Portland
200 S.W. Market Street
Suite 1750
Portland, OR 97201-5718
503.227.7400

Anchorage
510 L Street
Suite 500
Anchorage, AK 99501-1959
907.277.1900

New York
120 West 45th Street
New York, NY 10036-4041
212.832.8300

Washington, D.C.
1666 K Street, NW
Suite 300
Washington, D.C. 20006-1228
202.912.2000

Madison, WI
One East Main Street
Suite 201
Madison, WI 53703-5118
608.663.7460

Hong Kong
35th Floor, One Exchange
Square
8 Connaught Place
Central, Hong Kong
852.2292.2000

Singapore
50 Raffles Place
#17-04 Singapore Land Tower
Singapore 048623
65.6538.1756